Opening Statement of Dr. Edward Amoroso

Congressional Hearing on the Impact of Salt Typhoon and Cyber Threats to U.S. Critical Infrastructure

April 2, 2025 – 10:00 AM

Chairperson, Members of the Committee,

Thank you for the opportunity to speak with you today on this urgent and consequential topic. My name is Dr. Edward Amoroso. I serve as CEO of TAG Infosphere, a cybersecurity research and advisory firm. I am also a Research Professor at NYU, and prior to this, I served as Senior Vice President and Chief Information Security Officer for AT&T, where I led efforts to protect one of the world's largest telecommunications networks.

For over three decades, I have worked at the intersection of national security, critical infrastructure, and cybersecurity. I've seen the threat landscape evolve dramatically—but never as quickly or as dangerously as it is today.

The recent actions by the Chinese state-sponsored group Salt Typhoon represent not just another chapter in the long story of cyber espionage—they are a turning point. The targeting of our telecommunications infrastructure and the real-time collection of sensitive data on U.S. political leaders must be recognized for what it is: a full-spectrum assault on the trust and integrity of our democratic systems.

We will not solve this challenge by playing defense alone. We cannot rely solely on reactive "damage control" strategies that wait for the next breach before moving. Instead, we must fundamentally shift our approach. And I believe this pivot begins with **research and development**, with a bold, national investment in **artificial intelligence-driven cybersecurity**.

Here's why:
Our adversaries are not waiting. They are actively integrating AI into their offensive cyber arsenals—using machine learning to automate reconnaissance, exploit development, and the coordination of persistent, targeted attacks. If we do not respond in kind with equal or greater sophistication, we risk being outmatched not just occasionally, but systemically.

The United States must lead in building **AI-powered cybersecurity systems** that can anticipate, detect, and autonomously mitigate emerging threats to critical infrastructure. This means embracing **deep learning**, **behavioral analytics**, and **real-time adaptive controls** that can outpace the stealth and speed of AI-guided adversaries.

To do this, we need to create the conditions for sustained innovation. That means enabling **collaboration between industry, government, and academia**. The model for our future defense must be one of open, strategic alignment—not fragmented or siloed efforts.

The telecommunications sector, for example, stands at the front lines of this cyber war. But it cannot defend itself alone. Congress must ensure that federal cybersecurity agencies are not only coordinated with one another but integrated with private sector operations. Information sharing must become operational, not aspirational.

Further, we need to take legislative steps to encourage **proactive** defense strategies, including programs to fund AI R&D for critical infrastructure protection, to support workforce development in AI and cybersecurity, and to modernize policy frameworks that still reflect a pre-AI threat model.

To summarize:

- **AI is not just a tool—it is the new terrain** of cybersecurity.
- **Adversaries will use it**—and already are.
- **We must match and exceed them**—with urgency, coordination, and innovation.

Let's not wait for the next Salt Typhoon to show us what we failed to anticipate. Let's build the capability to see it coming—and stop it—before it even begins.

Thank you. I look forward to your questions.